

**Disclaimer**

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for ProCurve Networking products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. ProCurve Networking shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

© Copyright 2006, 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

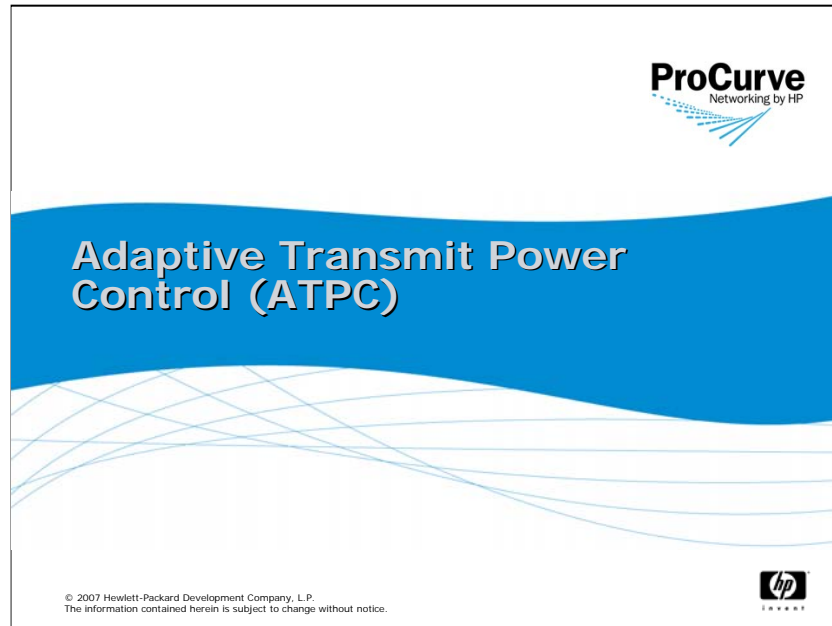
Objectives



- Describe how you can use adaptive transmit power control (ATPC) to minimize interference and maximize channel coverage.
- Explain how you can use group configuration to simplify the deployment and management of multiple access points (APs).
- Explain the uses for Web authentication (Web-Auth) and configure it for a wireless LAN (WLAN).
- Configure AP authentication (802.1X) on the AP 530 so that it can authenticate to a network edge device.
- Add a Simple Network Management Protocol version 3 (SNMPv3) user on the Access Point (AP) 530.
- Explain how the sFlow agent on the AP 530 samples and polls traffic from the Ethernet interface and the two radios.
- Describe how you can use MAC lockout to prevent a station from connecting to the AP.
- Explain how the client de-authentication feature forces a station to end its session and re-authenticate to the AP 530.
- Explain how to use the probe table in conjunction with ProCurve Mobility Manager (PMM).

Rev 1.2

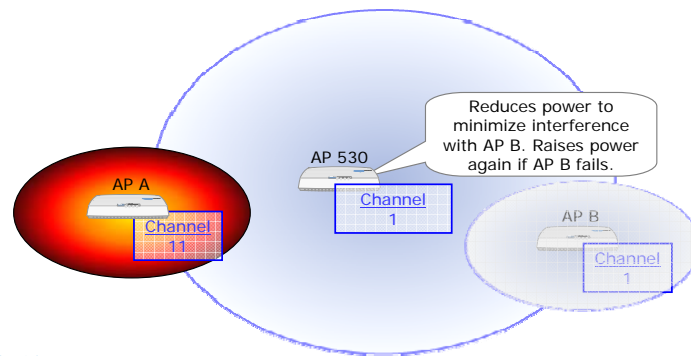
3



Adaptive Transmit Power Control (ATPC)



- Radio automatically reduces transmit power to:
 - Minimize interference with radios using the same channel
 - Maximize channel coverage
- Radios raise transmit power again to compensate for a failed neighbor.



Rev 1.2

5

Adaptive Transmit Power Control (ATPC)

Even when you carefully design cell coverage and assign neighbor APs non-overlapping channels, AP radios may be able to “hear” other AP radios that are using the same channel. This interference means that multiple AP radios and their associated stations are sharing the same transmission medium, decreasing overall throughput.

If you enable the Adaptive Transmit Power Control, or ATPC, feature, a radio can reduce its transmit power to minimize interference, while simultaneously maximizing channel coverage. When the radio detects interference, it changes its power level based on your settings.

An ATPC-enabled radio can also provide self-healing: if a neighboring AP is using the same channel and fails, the ATPC-enabled radio can boost its power to compensate. Of course, you must physically design your wireless network so that the APs are placed in close enough proximity to provide failover for each other. You must also configure ATPC appropriately so that the radio adjusts its power for that neighboring AP.

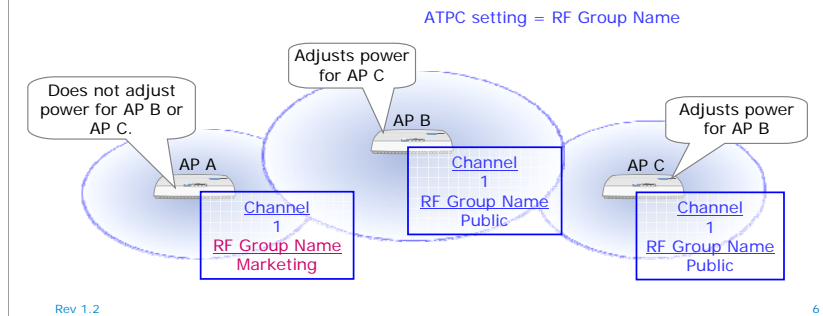
When planning redundancy for APs, you should keep in mind that an ATPC-enabled radio will not boost its transmit power to exceed its configured transmission level. On the AP 530, you will recall, you set the radio transmit power by configuring the **Tx Power Reduction** option. Calculated in dB, this setting is deducted from the maximum power level permitted for a channel in a particular country.

ATPC-Enabled Radio



You can configure a radio to adjust its transmit power in response to:

- AP radios that use the same channel and have the same RF Group Name
- AP radios that use the same channel and support the same SSIDs
- All AP radios that use the same channel



ATPC-Enabled Radio

When configuring ATPC, you must determine the neighbors to which a radio responds. You can configure a radio to adjust its transmit power in response to:

- Only AP radios that use the same channel and have the same **RF Group Name**—one of the ATPC settings that you configure for a radio
- Only AP radios that use the same channel and support the same Service Set Identifiers, or SSIDs
- All AP radios that use the same channel

In the example, the radios are configured with an **RF Group Name**: they will adjust their transmit power for other AP radios that use the same channel and have the same **RF Group Name**. As you can see, the AP B and AP C radios have the same **RF Group Name**. The AP B radio adjusts its transmit power for the AP C radio, and the AP C radio adjusts its power for the AP B radio.

The AP A radio, on the other hand, has a different **RF Group Name**, so it will not adjust its power for AP B or AP C.

Using the **RF Group Name** is the easiest way to ensure that the radios are adjusting their power for the appropriate radios that are in close proximity. However, you can allow radios to adjust their power for other AP radios that are using the same channel and support the same SSIDs. There is an example of this option later in this presentation.

You can also configure a radio to adjust its power in response to all AP radios on the same channel. You might select this setting if:

- Your wireless network includes APs that do not support ATPC.
- The AP 530 is in close proximity to another company's AP.

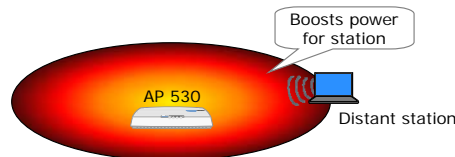
In this case, you must activate the **Avoid Neighbor APs** option—I'll show you how to do that later in this presentation.

Adaptive Mode



Determines if the AP 530 adjusts radio power based on audible APs or both audible APs and stations:

- AP only
 - Power is reduced to just reach the nearest AP.
 - Power reductions apply to all traffic, including beacons.
 - Use in dense deployments to encourage stations to associate with the nearest AP and to decrease contention.
- AP + Clients
 - Power is reduced to just reach the nearest AP but can be raised again to accommodate a more distant station.
 - Power reductions apply to traffic but not to beacons.
 - Use in less dense deployments to fill in potential gaps in coverage.



Rev 1.2

7

Adaptive Mode

You must determine whether the AP 530 adjusts its power based only on audible APs or based on both audible APs and stations (or clients).

If you select **AP** for the adaptive mode, the AP 530 reduces radio power so that it can just reach the nearest AP. The AP 530 sends both beacons and data frames at this power level.

You should select this setting for environments where coverage is good but contention must be reduced. This option encourages stations to associate with the nearest AP.

If you select **AP + Clients** for the adaptive mode, the AP 530 reduces the power for data transmissions to the level necessary for just reaching the nearest AP. However, the AP 530 sends beacons at full power, allowing stations that would otherwise not hear the beacons to associate with one of the radio's SSIDs. The AP 530 also temporarily raises its power high enough to transmit data to these more distant stations. Reducing power for most data transmissions minimizes interference while transmitting beacons at full power maximizes the radio's coverage area.

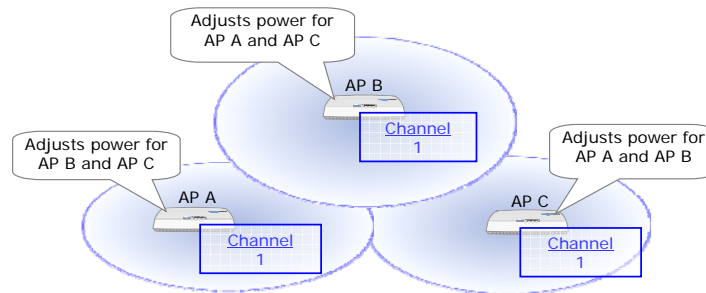
You should select the **AP + Clients** option for environments where complete coverage is a concern. Such an environment might feature a low-density of APs or obstacles that create holes in the coverage area.

Avoid Neighbor APs Option



Reduces a radio's transmit power in response to *all* neighbor APs using its channel:

- Don't set the RF Group Name; it has no effect.
- Use AP + Clients adaptive mode to prevent stations from losing their connection to this radio's WLAN.



Rev 1.2

8

Avoid Neighbor APs Option

You should select the **Avoid Neighbor APs** option if you want the radio to reduce transmit power in response to *all* AP radios detected on its channel. In effect, the **Avoid Neighbor APs** option helps you to be a good neighbor in a congested wireless environment: the AP 530 radio uses the lowest signal level possible to minimize interference with your neighbors.

When you select this option, you cannot configure an **RF Group Name**. The **RF Group Name** is irrelevant because the radio is configured to adjust its power level for all AP radios using its channel.

You should use the **AP + Clients** adaptive mode in conjunction with the **Avoid Neighbor APs** option. Otherwise, some stations might lose their connection to the AP 530 radio. Because you selected the **AP + Clients** adaptive mode, however, the AP 530 radio transmits beacons at full power so that it still provides maximum coverage for *your* WLAN.

Guidelines for Using ATPC



- Configure ATPC for each radio.
- Space APs closely enough to provide full coverage at *reduced* power.
- If you want ATPC to provide self-healing, space APs so that if one AP fails the remaining neighbor APs can provide full coverage.
- For IP phones and other devices that use aggressive roaming controls, use the AP adaptive mode.
- The power adjustment period varies, depending on the Adaptive Mode:

Adaptive Mode	Increasing Power	Decreasing Power
AP	Waits 2 minutes	Waits 2 minutes
AP + Clients	Adjusts power once per second	Waits 2 minutes

Rev 1.2

9

Guidelines for Using ATPC

You configure ATPC separately for each radio.

ATPC functions best for APs that are spaced relatively close together. Remember that ATPC allows radios to *reduce* power; a radio cannot increase its power beyond its full transmit power (although you can attach an external antenna to amplify the signal). If you deploy APs so far apart that their radio signals barely reach each other at full power, ATPC serves no purpose: interference is already at a minimum. Worse, wireless signals tend to fluctuate in strength so that the coverage area undoubtedly has holes from time to time.

To provide failsafe coverage, you should space APs closely enough together to provide full coverage even at reduced power. When signals are strong, ATPC comes into play, allowing radios to dynamically reduce power and minimize interference. If signal strength falls, radios can increase their transmit power until they once again provide full coverage.

Spacing APs closely together also enables ATPC to provide self-healing. You should space the APs so that if any one AP fails, the remaining AP radios can raise their power high enough to once again provide full coverage.

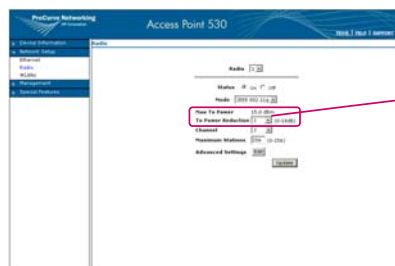
If you are using IP phones and other devices that employ aggressive roaming controls, you should select the **AP** mode. Such devices are extremely sensitive to variations in transmit power and do not interoperate well with APs that use the **AP + Clients** mode.

The power adjustment period depends on which **Adaptive Mode** you select. If the **AP** mode is selected, the radio will wait approximately two minutes after detecting interference before increasing or decreasing power. With the **AP + Client** mode, however, the radio must increase its power more rapidly to hold on to distant stations. If this mode is selected and power must be increased, the radio changes its power once per second. The radio will decrease its power more slowly; it will wait approximately two minutes to start decreasing power.

Main Configuration Steps



1. Enable ATPC for a radio.
2. Choose the adaptive mode.
3. Optionally, configure an RF Group Name.
4. Optionally, enable Avoid Neighbor APs.
5. Set the maximum power reduction:
 - Select a value between 0 and 18 dB.
 - This value is combined with the static reduction configured for the radio.



Tx Power Reduction 3 dB
 + Tx Power Reduction Limit 11 dB
 Total Power Reduction Possible 14 dB

Rev 1.2

10

Main Configuration Steps

Configuring ATPC is a straightforward process. You enable the feature for a particular radio and then select the adaptive mode—either **AP** or **AP + Clients**.

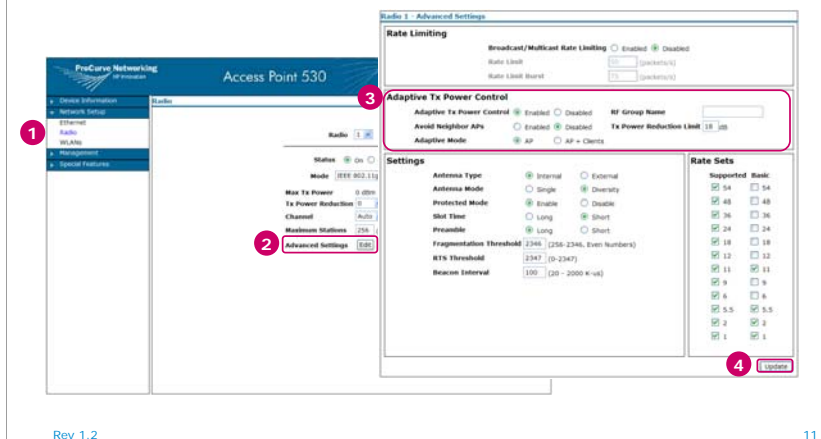
The next two steps are optional: If you want the radio to adjust its power for the AP radios you include in a group, configure the **RF Group Name**. If you want the radio to react to *all* audible AP radios using its channel, select the **Avoid Neighbor APs** option. If you want the radio to respond only to the AP radios that support the same SSIDs, do not configure either of these options. (This is the default setting.)

Finally, you set the maximum power reduction in dB. The default value is 18 dB. At this setting, a radio can decrease its transmit power by any value between 0 and 18 dB. The ATPC reduction is combined with whatever static reduction you manually set for the radio. In the example, the radio's **Tx Power Reduction** is set to 3 dB, which permanently decreases the radio's maximum transmit power (for this channel in this country) to 15 dBm. If you then enable ATPC and set the **Tx Power Reduction Limit** to 11, the AP can dynamically set the power for this radio between 4 dBm and 15 dBm, depending on current conditions.

Configuring ATPC



On the Radio screen, click the Edit button for Advanced Settings.



Configuring ATPC

To configure the ATPC settings for a radio, select **Network Setup > Radio**. On the **Radio** screen, click the **Edit** button for **Advanced Settings**. (The **Edit** button is enabled after you enable the radio itself.)

When the **Advanced Settings** screen is displayed, select the **Enabled** option for **Adaptive Tx Power Control**. All of the ATPC options are then enabled.

You can optionally configure an **RF Group Name** or select the **Avoid Neighbor APs** option. If you do not configure either of these options, the radio will react only to AP radios that support the same SSIDs.

Then, choose the **Adaptive Mode** and configure the **Tx Power Reduction Limit**.

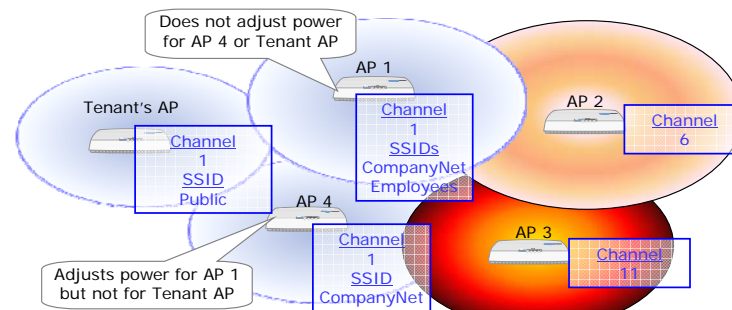
Finally, click the **Update** button to save your configuration to the startup-config.

ATPC Use Model—Airport



The APs should use the *least* power necessary to provide coverage for *two* WLANs:

- Adaptive Mode = AP
- RF Group Name = none
- Avoid Neighbor APs = Disabled



Rev 1.2

12

ATPC Use Model—Airport

This slide shows a customer use model for implementing ATPC in an airport. In this area of the airport, the IT staff has set up four APs. One of the airport tenants has also set up its own AP to provide wireless services for its customers.

In setting up ATPC for the radios on its four APs, the airport IT staff wants to use the least amount of power necessary to provide coverage for two WLANs—CompanyNet and Employees. The **AP** setting has been selected for **Adaptive Mode**, so none of the radios will factor in clients when adjusting transmit power. The radios will adjust power equally for both beacons and data transmissions.

The radios have not been assigned an **RF Group Name**, and the **Avoid Neighbor APs** option is disabled. Consequently, the radios will adjust their transmit power only for AP radios that use the same channel and support the same SSIDs.

As you can see, the AP 1 radio, the AP 4 radio, and the tenant's AP are all using the same channel. The AP 2 and AP 3 radios are using different channels so ATPC does not affect them.

Because the tenant's AP does not support the same SSIDs, neither the AP 1 radio or the AP 2 radio will adjust its power for this AP. This behavior falls in line with the airport administration's goals: it wants full coverage for its own WLANs; it does not care about the tenant's WLAN.

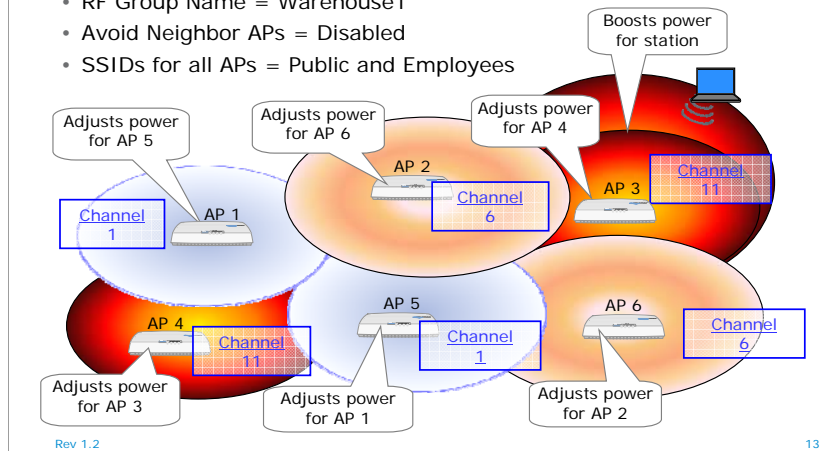
The AP 4 radio supports a subset of the SSIDs on the AP 1 radio. Therefore, the AP 4 radio will adjust its power for the AP 1 radio. However, the AP 1 radio will not adjust its power for the AP 4 radio because it does not support all the SSIDs that the AP 1 radio supports. Again, the configuration satisfies this company's goals: the radios should provide full coverage for *both* WLANs.

ATPC Use Model—Warehouse



This warehouse has potential coverage gaps:

- Adaptive Mode = AP + Clients
- RF Group Name = Warehouse1
- Avoid Neighbor APs = Disabled
- SSIDs for all APs = Public and Employees



ATPC Use Model—Warehouse

This slide shows a customer use model for implementing ATPC in a warehouse, which presents unique challenges for a company trying to set up a wireless network.

In a warehouse, items are typically stored on a temporary basis. Over time, items are stacked in different places and in various configurations. Shelves may be stacked to the ceiling one day and moved to an entirely new location another day.

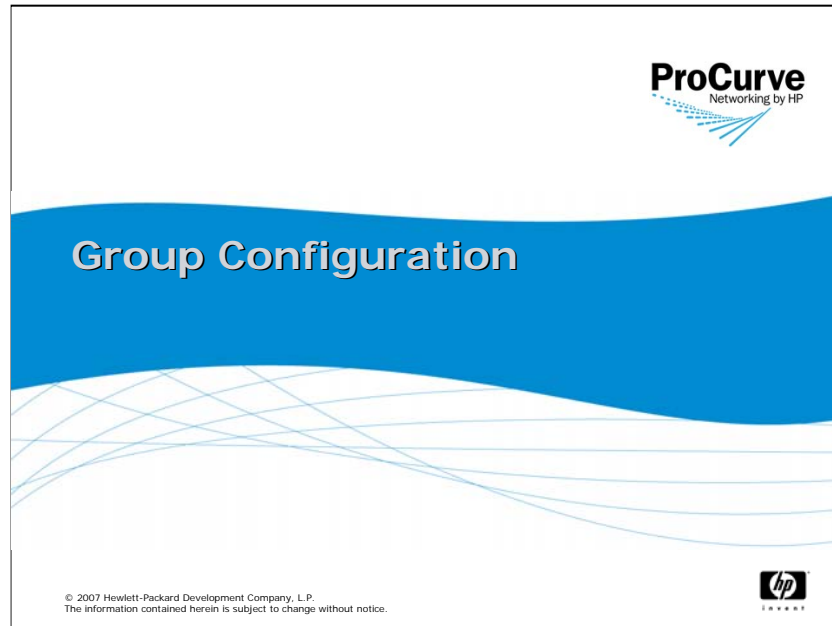
Users are also extremely mobile, riding fork lifts and other machinery throughout the warehouse.

To provide the best possible wireless coverage for this changing landscape, the network administrator configured ATPC for all AP radios, selecting **AP + Clients** as the **Adaptive Mode** and configuring **Warehouse1** as the **RF Group Name**. The **Avoid Neighbor APs** option is disabled, and all the AP radios support the same SSIDs—Public and Employees. Because the radios are in the same RF group, however, they will not consider SSIDs when adjusting radio power.

The AP 1 and AP 5 radios are using the same channel. Both will adjust their power for each other, also taking into account stations so that stations will not lose a connection if signal levels drop.

Likewise, the AP 2 and AP 6 radios are using the same channel and will adjust their power for each other as well as for stations.

Finally, the AP 3 and AP 4 radios adjust power for each other. As you can see, the AP 3 radio is boosting its power for a distant station. This illustrates the behavior of all the AP radios when a distant station associates with one of their SSIDs.

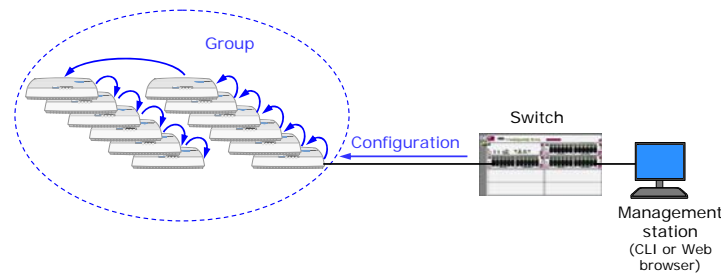


Group Configuration



Eases deployment and management of APs in a small-to-medium network when all APs require the same basic configuration:

- You configure any AP, using:
 - Command line interface (CLI)
 - Web browser interface
- The configuration is automatically shared with other APs in the group.



Rev 1.2

15

Group Configuration

Some small-to-medium businesses find themselves in an uncomfortable position—too small to purchase a Simple Network Management Protocol, or SNMP, solution to manage many APs centrally, but large enough that network administrators find it tedious to configure the number of APs required for the network.

For companies that have a group of APs requiring the same basic configuration, the new group configuration feature provides a good solution to this problem. Using this feature, you can configure any AP and have that configuration shared with multiple APs.

Configuring the group is easy. You simply configure any AP in the group exactly as you would if the AP were not part of a group. You can configure the AP through the command line interface, or CLI, or the Web browser interface.

The only difference with group configuration is that a configuration on that one AP is shared among all group members. For example, when you configure a WLAN on the AP or add a user account to its local database, you've completed the task for all APs in the group.

Which Parameters Are Shared?



- Shared parameters, called the *Group Configuration Parameter Block*:
 - WLAN
 - Global Web-Auth settings
 - Local RADIUS database
 - Management passwords
 - Clear and Reset button settings
 - SNMP
 - Local MAC-Auth tables
 - MAC lockout list
 - Quality of Service (QoS)
 - Probe table
 - Filters
 - SNTP
 - LLDP enable or disable
- Parameters individual to each AP:
 - IP settings
 - Management and untagged VLANs
 - Radio settings
 - Wireless bridge (or WDS connection)
 - Access to the CLI and Web browser interface

Rev 1.2

16

Which Parameters Are Shared?

Members of a group have identical settings for the parameters that are part of the Group Configuration Parameter Block. For example, to support the same wireless network, APs must, of course, enforce the same WLAN settings. And to allow a user to connect to the wireless network no matter where he or she happens to be at the moment, all APs must share RADIUS database settings and local MAC-Auth tables. Other shared settings help to create a consistent experience for wireless users (and for managers configuring the APs).

The slide lists the Group Configuration Parameters:

- WLAN settings
- Global Web-authentication, or Web-Auth, settings (as well as Web-Auth settings for a particular WLAN)
- Local RADIUS database
- Management passwords
- Clear and Reset button settings
- SNMP settings
- Local MAC-Auth tables
- MAC lockout lists
- Quality of Service, or QoS
- Probe table
- Filters, which include inter-station blocking and wireless management blocking
- Simple Network Time Protocol, or SNTP
- Link Layer Discovery Protocol, or LLDP

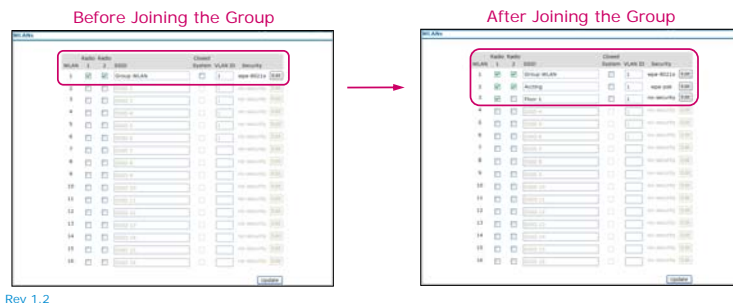
Each AP 530 also has unique settings. As you would expect, each has its own IP address. Other parameters individual to each AP 530 include:

- Management virtual LAN, or VLAN, and untagged VLANs
- Radio settings
- Wireless bridge (or WDS) settings
- Management access to the CLI or Web browser interface

Synchronization Among Group Members



- Each member tracks other members and their age, or time in group.
- The AP with the oldest membership serves as the reference point.
- Synchronization occurs when:
 - An AP joins or leaves the group
 - A group parameter is saved to the startup-config file on any AP in the group (using write memory in the CLI or applying changes in the Web browser interface)



Rev 1.2

17

Synchronization Among Group Members

Members of a configuration group store a list of all other members in the group and their age, or time since joining the group.

The AP 530 with the oldest membership acts as the reference point for the entire group. When members of the group synchronize their configurations, they synchronize to the reference point. If the reference point leaves the group, the remaining AP with the oldest membership becomes the new reference point. The reference point serves as the touchstone for synchronization, but members of the group have a peer-to-peer relationship.

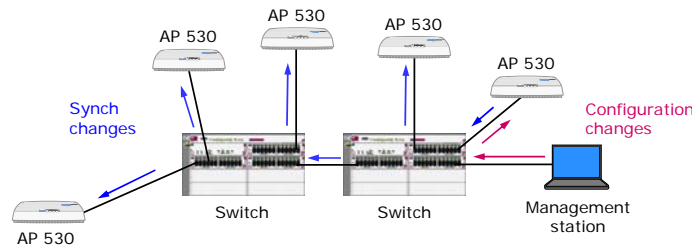
Synchronization occurs when an AP 530 joins or leaves the group or when a group parameter is changed and saved to the startup-config file on any of the AP 530s. The change can be saved by entering **write memory** in the CLI or by applying changes in the Web browser interface.

The slide shows the WLAN screen for an AP 530 before it joined a group and after it joined a group. Initially, the AP 530 supported a single WLAN. The group of APs, on the other hand, supported three WLANs. When the AP 530 was added to the group, it automatically received the configurations for the other two WLANs—the network administrator did not have to manually configure the two additional WLANs on the AP.

Secured Transmissions Among Group Members



- APs synchronize over the Ethernet connection, using Secure Sockets Layer (SSL) to protect the transmissions.
- Synchronization may take up to 1 minute, depending on the number of APs in the group and network latency.
- Each AP broadcasts its up status every 10 seconds.
- If an AP does not send a broadcast for 70 seconds, the other members remove it from the group.



Rev 1.2

18

Secured Transmissions Among Group Members

The APs synchronize their configurations over the Ethernet network, using Secure Sockets Layer, or SSL, connections. SSL guards against eavesdroppers or hackers that might try to discover your AP 530 settings.

The synchronization time depends on the number of APs in the group and network latency. The more APs, the more time is required, and networks with a high volume of traffic will, of course, have a slightly longer synchronization time. Even in a busy network and a group that contains 12 members, however, complete synchronization should not take more than 1 minute.

Each AP broadcasts its up status every 10 seconds. All the APs in the group listen for these broadcasts so that they can detect new members and track the status of existing members. If an AP does not send this broadcast for 70 seconds, the other APs in the group remove it from their list of members.

Group Configuration Guidelines



- APs must be the same model.
- ProCurve recommends that all APs run the same software version.
- All group members must be on the same subnet and have the same management VLAN.
- A subnet can include multiple groups—each identified by a different group name.
- The group cannot extend over a wireless bridge (or WDS connection).

Rev 1.2

19

Group Configuration Guidelines

When setting up group configuration, you must ensure that all APs are the same model. Using APs that are the same model should not be restrictive: you should purchase only the AP models for your region—either Worldwide (WW) or North America (NA).

In addition, ProCurve recommends that all APs use the same software version. Again, this should not be restrictive because best practices dictate that you upgrade all your APs to the latest release of the software. If a group includes APs that are running different software versions, however, the APs will share settings for all Group Configuration Parameters that have the same name. If a parameter name is changed in a new release, the APs will simply not share that setting.

Group members must also be on the same subnet. For the purposes of group configuration, the APs must have their management IP addresses on the same subnet, and accordingly, they must use the same management VLAN ID.

A single subnet can have multiple configuration groups, which are distinguished by different group names. You might choose this design when a subnet includes more than the recommend number of APs for a group or when you want certain APs to support different WLANs.

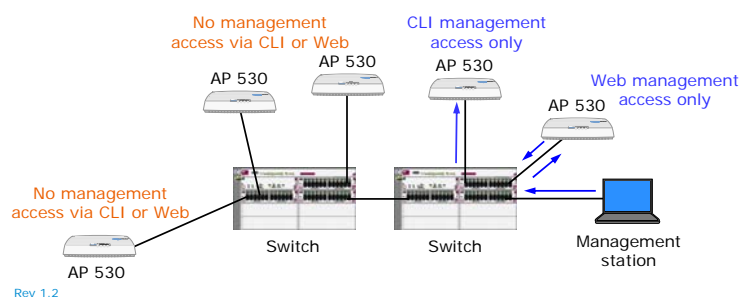
In addition, the group cannot extend over a wireless bridge, even though two APs connected by a wireless bridge are on the same subnet. (Note that a wireless bridge is called a WDS connection on the AP 530.)

In fact, you should not enable group configuration for an AP 530 that supports a wireless bridge. If someone changes the security settings for WLAN 1, the change could affect the wireless bridge, possibly breaking it.

Recommendations for Group Configuration



- A group can support up to 12 APs (recommended).
- Limit management access so that network administrators do not inadvertently make conflicting changes:
 - Enable CLI access on only one AP 530
 - Enable the Web browser interface on only one AP 530
- If an AP is already configured with the settings you want for the group, enable group configuration on that AP first so that it functions as the reference point.



Recommendations for Group Configuration

In theory, a group can have any number of members, but ProCurve Networking recommends that a group include a maximum number of 12 members.

Because you can change the group configuration by accessing a management interface on any of the group members, you should take some precautions to protect against configuration conflicts. The configuration entered last overrides previous configurations, but if two network administrators attempt to configure settings, the last configuration may not be the correct one.

For example, you may want to restrict access to the management interfaces of all but two of the APs in a group. On one AP, you could permit access to the Web browser interface; on the other AP, you could permit access to the CLI. Then, you could instruct network administrators to configure the AP group from the Web browser interface, unless it becomes unavailable for some reason. As a backup, you would still have access to the second AP through the CLI and could easily enable access to this AP's Web browser interface if necessary.

If you have configured one AP with the settings you want for the group, enable the group configuration feature on that AP first. This ensures that, as the oldest member of the group, the AP becomes the reference point. When you add members to the group, they will then receive the settings that were configured on the first AP before the group was created. (After this initial setup, it doesn't really matter which AP functions as the reference point.)

If you create the group before you configure group configuration parameters on any of the APs, you don't need to worry about which AP becomes the reference point. In this case, you would enable the group configuration feature on all the APs, thereby establishing the group. You would then configure your settings on any AP in the group, and the settings would be shared among the group members.

Main Configuration Steps



1. Specify the Group Name.
2. Optionally, specify a Member ID to identify the AP 530 by name.
 - The AP 530 is also identified by its MAC and IP addresses.
3. Enable Group Configuration.
4. Update your changes.

Rev 1.2

21

Main Configuration Steps

You must set up group configuration on each AP 530 that you want to include in a group. Configuration is easy and includes only three steps for each AP: you must specify the **Group Name**, which must be the same on each AP in the group. You must enable **Group Configuration**, and finally, you must update your changes.

To easily identify the members of the group, you can also configure a member ID, or name, for each AP. However, this step is not required because each AP is identified in the list of group members by both its MAC and IP addresses.

Set Up Group Configuration



Select Management > Group Configuration.

The screenshot shows the 'Group Configuration' page in the ProCurve Access Point 530 web interface. The left sidebar (1) contains navigation options: Device Information, Network Setup, Management, Local MAC Authentication, Web Authentication, SNMP, Group Configuration (selected), AP Authentication, AP Access, System Maintenance, and Special Features. The main content area (3) has a 'Group Configuration' section with a radio button for 'Enabled' (selected) and a 'Disabled' option. Below this are fields for 'Group Name' (Group 1) and 'Member ID' (Group Leader). A 'Members' table (2) lists the group members with columns for ID, MAC Address, and IP Address. The table shows 'Building 2' with MAC address 00-14-C2-A5-B9-02 and IP address 10.1.1.228, and 'Group Leader' with MAC address 00-14-C2-A5-B9-03 and IP address 10.1.1.238. A red bracket (4) labeled 'Group Members' points to the table. An 'Update' button is at the bottom right.

ID	MAC Address	IP Address
Building 2	00-14-C2-A5-B9-02	10.1.1.228
Group Leader	00-14-C2-A5-B9-03	10.1.1.238

Rev 1.2

22

Set Up Group Configuration

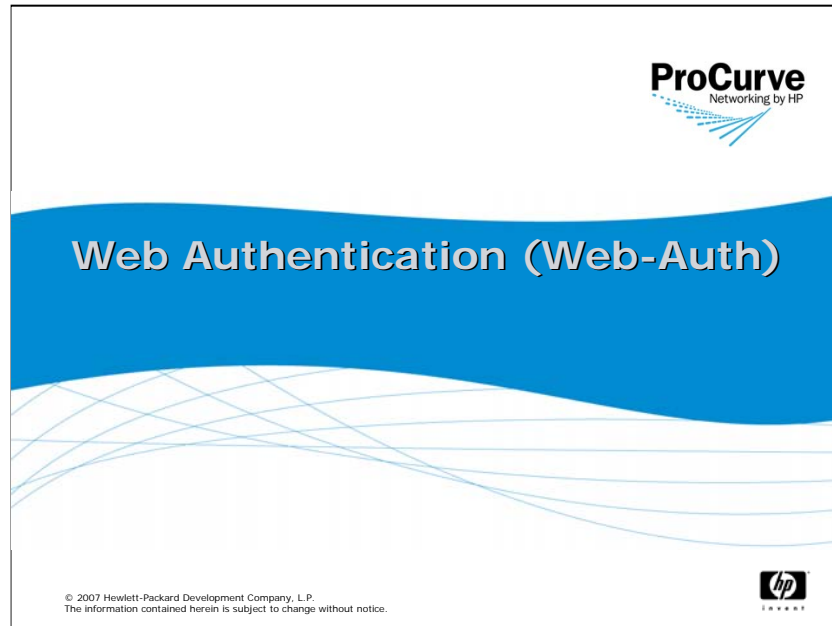
To configure this feature, select **Management > Group Configuration** and then select the **Enabled** option for the **Group Configuration** field.

In the **Group Name** field, enter the name you want to assign this group. You must enter the same group name on all the APs that you want to be part of the same group.

To identify this particular AP with a name, configure the **Member ID** field.

Click the **Update** button to commit your changes to the startup-config.

The AP 530 immediately begins to send broadcast messages and listen for other APs' broadcast messages in return. When you have configured other members, refresh the screen to view the members list.



Web-Auth



- Authenticates users but does *not* require:
 - 802.1X support on the wireless client
 - Special configuration of the wireless client
- Typically used for:
 - Guest access
 - Courtesy or public networks
 - Small-to-medium organizations

Rev 1.2

24

Web-Auth

Web authentication, or Web-Auth, authenticates users trying to access your wireless network but does not require 802.1X support on the wireless client. In addition, users do not have to configure their wireless client with any security settings.

For these reasons, Web-Auth is typically used for environments where the company does not control the users' network equipment. For example, companies often need to provide wireless access for guests as well as employees. These guests use a variety of equipment and have different technical aptitudes and skills. Some guests may have the latest laptops and run up-to-date software. Other guests, however, may have older laptops and may not have updated their software. As a result, their laptops may not even support 802.1X. Likewise, some guests will know how to configure their wireless client with different security options, but other guests may not be comfortable completing this task.

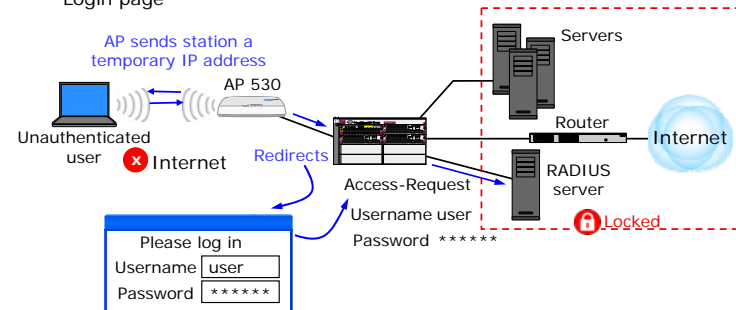
Companies that provide courtesy or public networks have the same problems. They must make it easy for users to connect to the wireless network—regardless of the users' equipment and computer skills.

Some small-to-medium organizations might also choose Web-Auth because they have older equipment or allow their employees to use their own equipment.

Web-Auth Process



- User associates to the WLAN.
- AP 530:
 - Sends the user's station a temporary IP address
 - Intercepts station's traffic, redirecting browser to the Login page
- AP 530 handles authentication:
 - Internal RADIUS server
 - External RADIUS server (PAP)
- Authenticated users gain complete access—limited by other controls.



Rev 1.2

25

Web-Auth Process

With the first release of the AP 530, you implemented Web-Auth through the edge switch in addition to whatever other wireless security you configured on the AP 530. With the 2.0 update, Web-Auth is now implemented on the AP 530 itself.

In the simplest configuration for Web-Auth, no security is required for the 802.11 association process. A user can simply open a wireless utility, select the WLAN, and associate to it.

After the station associates to a WLAN, the AP 530 provides the station with a temporary IP address and blocks the user's traffic until that user completes the Web-Auth process. When the user opens a browser, he or she is immediately redirected to the Web-Auth Login page, which is designed to help the user log in by submitting a username and password or by clicking the **Guest** button, as described on the next slide.

The AP 530 sends the login credentials to its internal RADIUS server or to the external RADIUS server, depending on your configuration. If the credentials match those stored on the RADIUS server, the user is granted access to the network resources to which he or she has rights.

Two Types of Web-Auth Logins



- User Login
 - User accounts configured on the internal or external RADIUS server.
 - When users are redirected to the Login page, they enter their username and password.
 - The user's credentials must match those stored on the RADIUS server.
- Guest Login
 - Special guest username and password configured on the AP 530.
 - When redirected to the Login page, the user simply presses a Guest button.
 - The AP 530 submits the guest username and password to the RADIUS server.
 - Multiple users can log in using this one account.

Rev 1.2

26

Two Types of Web-Auth Logins

You can configure two types of logins for Web-Auth users: User Login and Guest Login.

User Login

The User Login supports traditional user accounts, which are configured on the internal or external RADIUS server. Each user has a unique username and password.

With the User Login, users are redirected to the Web-Auth Login page, which prompts them to enter their username and password. The AP 530 then submits these credentials to the RADIUS server for verification.

Guest Login

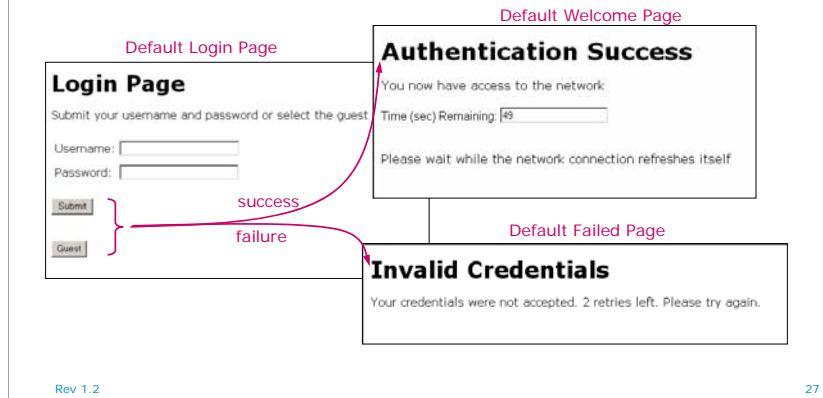
With the Guest Login, on the other hand, the user is not required to enter a username or password. When the guest user is redirected to the Login page, he or she simply clicks the Guest button (as shown on the next slide).

To facilitate the Guest Login, you configure a guest username and password for Web-Auth on the AP 530. When a user clicks the Guest button, the AP 530 submits this username and password on behalf of the user. The matching account you configure on the RADIUS server must support multiple logins.

Customizable Web Pages



- Login, which prompts the user to enter login credentials or press the Guest button
- Welcome, which reports the login was successful
- Failed, which explains that the login was unsuccessful



Customizable Web Pages

The AP 530 provides several Web pages to guide users through the process of logging in. You can customize three of these Web pages: the Login page, the Welcome page, and the Failed page.

Login Page

As you would expect, the Login page prompts the user to enter his or her login credentials or to press the Guest button.

Welcome Page

If the login is successful, the Welcome page is displayed. In addition to reporting that the login was successful, the Welcome page prompts the user to wait while the network connection is “refreshed.” During this time, the station releases the temporary IP address it received from the AP 530 and receives an IP address from the network DHCP server. This second IP address is part of the address range for the VLAN assigned to the Web-Auth WLAN.

For example, you might assign VLAN 8 to the WLAN and then set up the DHCP server so that VLAN 8 has the IP address range 10.1.8.0 /24. In this case, the station might receive the IP address 10.1.8.50.

After receiving an IP address for the appropriate VLAN, the station can begin to access the network resources to which the user has rights. I’ll discuss ways in which you can configure rights—as well as other security considerations—on the next slide.

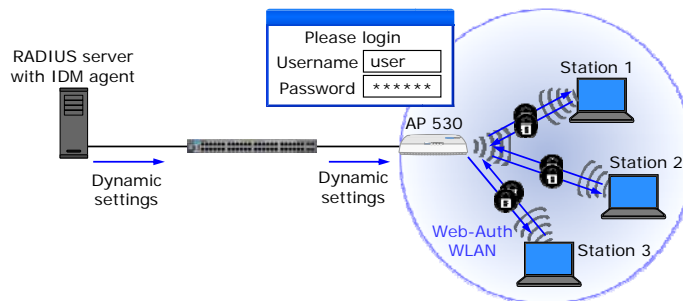
Failed Page

Of course, if the login credentials the user enters do not match those stored on the RADIUS server, the login fails, and the Failed page is displayed. By default, the user can make three attempts to log in. In the example, the user has made one unsuccessful attempt and can try two more times.

Additional Security for Web-Auth



- Optional encryption:
 - Static Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)/WPA2 with Preshared Key (PSK)
- Dynamic, user-based settings, compatible with ProCurve IDM:
 - VLAN assignment
 - Access control lists (ACLs)
 - Rate limits



Rev 1.2

28

Additional Security for Web-Auth

Optional Encryption

Although Web-Auth controls access to your private network, wireless transmissions are vulnerable to any eavesdropper. The AP 530 supports optional encryption in Web-Auth WLANs to shore up security on the wireless side. You can choose either Wired Equivalent Privacy (WEP) or the far more secure Wi-Fi Protected Access, or WPA/WPA2.

In either case, however, the encryption key is static, and users must enter this key *before* they connect to the network and are redirected to the Login Web-Auth page.

After an authenticated user receives access to the network, you can control the user's access through the network infrastructure—for example, through a directory service or through access control lists, or ACLs, configured on the edge switch.

Dynamic Settings

The AP 530 can also accept and enforce dynamic settings configured on a RADIUS server, including:

- VLAN assignments
- Access control lists, or ACLs
- Rate limits

ProCurve Identity Driven Manager, or IDM, simplifies the configuration of access controls on the RADIUS server. The AP 530 includes an IDM agent, so you can use IDM to configure dynamic settings on the AP's internal RADIUS database at the same time that you configure policies for your entire network.

Guidelines for Configuring Web-Auth



- Roaming is not supported for Web-Auth users.
- Web-Auth configuration is shared among APs if group configuration is enabled.
- Web-Auth can be used in conjunction with MAC authentication.

Rev 1.2

29

Guidelines for Configuring Web-Auth

There are a few guidelines you should understand before you begin to configure and use Web-Auth. First, roaming between APs is not supported for Web-Auth users. If Web-Auth users move out of range from one AP 530 to another AP 530 that supports the same WLAN, they must re-enter their login credentials.

Second, if you are using the group configuration feature, Web-Auth settings are shared among members of a group.

Finally, you can use Web-Auth in conjunction with MAC authentication.

Main Configuration Steps



1. Configure the WLAN—SSID and VLAN ID.
2. Optionally, configure static WEP or WPA-PSK security.
3. Specify the RADIUS server.
4. Configure Web-Auth for the WLAN.
 - a. Enable Web-Auth.
 - b. Select a login type—User Login, Guest Login, or both.
 - c. Accept default settings for other options or customize them for your environment.
5. Optionally, configure a temporary IP address range.
6. Configure a guest account username and password if you are using Guest Login.

Rev 1.2

30

Main Configuration Steps

To configure Web-Auth, you first configure basic WLAN settings, such as the SSID and VLAN ID, which are always required for every WLAN. If you want to secure the transmissions between the AP 530 and each station, you can configure either static WEP or WPA-PSK. (You cannot select dynamic WEP or WPA with 802.1X.) If you want users to be able to access the login screen without first entering a password in their wireless client utility, you would skip this step.

Web-Auth, like 802.1X, enforces authentication to a RADIUS server, so you must specify either the internal or external RADIUS server.

Steps four to six involve configuring the new Web-Auth features. You must enable Web-Auth and select a login type—User Login, Guest Login, or both. You can then accept default settings for other options—such as the words that are displayed on Web-Auth pages—or customize them for your environment. You can also accept the default settings for the temporary IP address range or customize these settings for your environment. And if you are using the Guest Login, you configure a guest account.

On the next few slides, I'll go into the steps for configuring the new Web-Auth settings in more depth.

Configure the WLAN

The screenshot shows the ProCurve Access Point 530 configuration interface. The left sidebar has a menu with 'WLANs' selected (indicated by a red circle 1). The main area shows the 'WLANs' configuration table (indicated by a red circle 2). The table has columns for Radio, SSID, VLAN ID, and Security. The 'Security' column for the first row is highlighted with a red circle 3. An inset window shows the 'Security' configuration page for the selected WLAN. The 'Security Mode' is set to 'WPA-PSK' (indicated by a red circle). The 'WPA Versions' are set to 'Both'. The 'Enable pre-authentication' checkbox is checked. The 'Cipher Suites' are set to 'TKIP'. The 'Pre-Shared Key' field is empty. A red bracket on the right side of the inset window indicates 'Configure other settings'. A red arrow points from the 'Security Mode' dropdown to the text 'Optionally, select WPA-PSK or static WEP for the Security Mode'.

Rev 1.2

31

Configure the WLAN

To provide the context for configuring the Web-Auth settings, I'll quickly go over the initial steps for setting up a WLAN.

You access the **WLANs** screen by selecting **Network Setup > WLANs**. Then, enter the settings for the **SSID** and **VLAN ID** fields and enable the WLAN on Radio 1, Radio 2, or both. Click the **Update** button to apply the basic settings.

Next, click the **Edit** button.

If you want to secure the *wireless* transmissions for the Web-Auth WLAN, select either **WPA-PSK** or **static WEP** for the **Security Mode**. Then, configure the related settings, including the **Pre-Shared Key** for WPA or the **WEP Key** for static WEP.

Specify the RADIUS Server



Select the RADIUS Servers tab.

WLAN Configurations - SSID 1 - Radius Servers

Retransmit Attempts [0] (0-30)

Primary Server

Internal Server ☐

IP Address [0.0.0.0]

Port [1812]

Key []

MAC Address Format [No Delimiter xxxxxxxxxxxx]

Secondary Server

Internal Server ☐

IP Address [0.0.0.0]

Port [1812]

Key []

MAC Address Format [No Delimiter xxxxxxxxxxxx]

☐ Internal server as fail over

Update

Not supported for Web-Auth

Configure the RADIUS server settings for your network

Rev 1.2 32

Specify the RADIUS Server

Next, select the **RADIUS Servers** tab to configure these settings for the WLAN. You should specify if you want to use the internal server or an external server. If you use the internal server, you will also need to configure the usernames and passwords in the internal database (by clicking **Special Features > Local RADIUS**).

If you use an external server, you must supply the IP address on the RADIUS Servers screen and the key, if the RADIUS server requires a shared secret.

Note that the **Internal server as fail over** option is not supported for Web-Auth.

After you enter your settings, click the **Update** button.

Configure Web-Auth Settings for the WLAN

Select the Web Authentication tab.

WLAN Configuration - Guestonly - Web Authentication

Web Authentication ☒ Enabled ☐ Disabled

☐ Guest Login ☒ User Login

Redirect URL

Retry Limit

Login Welcome Failed

Default Text ☒

Title Text

Header Text

Footer Text

Descriptive Text

Update

Rev 1.2

33

Configure the three Web-Auth pages that can be customized

Customize text displayed on Login page.

Configure the Web-Auth Settings for the WLAN

You may have noticed that the **WLAN Configuration** screen now includes a **Web Authentication** tab. Select this tab to configure the Web-Auth settings for the WLAN.

Select **Enabled** and click **Update** to activate the Web-Auth options.

Next, select a login type. Select **User Login** if you want some users to enter a unique username and password. Select **Guest Login** if you want to simplify the login process for some users, allowing them to simply press the **Guest** button to gain access to the network. You can select both options for a WLAN.

You can then configure the **Redirect URL** option if you want to redirect users' Web browser to a particular Web page after they log in successfully. For example, you might want to redirect their Web browser to a page on your company's intranet.

You can also change the **Retry Limit**, which controls how many times a user can try to log in. The default setting is three, which means the user can make three attempts to enter the correct login credentials. You can specify a setting between one and nine for this option.

Then, if you want, you can customize the text that is displayed on the Login, Welcome, and Failed pages. For example, on the Failed page, you might want to provide an extension number for users to call if they cannot log in.

After you have configured the Web-Auth settings for this WLAN, click the **Apply** button.

Configure Global Web-Auth Settings—Temporary Address Pool



ProCurve Networking
Access Point 530

Web Authentication - Address Pool

Address Pool

Starting IP Address: 192.168.0.1

Subnet Mask: 255.255.240.0

Lease Time: 30 (sec)

Update

Rev 1.2

34

Configure Global Web-Auth Settings—Temporary Address Pool

As mentioned earlier, the AP 530 assigns each station a temporary IP address to use until the Web-Auth process is completed. To configure the address pool for temporary IP addresses, select **Management > Web Authentication > Address Pool**.

The **Address Pool** settings are global: they apply to the entire AP 530.

By default, the temporary IP address range is 192.168.0.0, starting with the address 192.168.0.1. The **Subnet Mask** is 255.255.240.0, or /20, which means there are 4,096 addresses available.

If you change this range of IP addresses, ensure that the range you specify is large enough to support all of the Web-Auth stations logging in to your network. Because the temporary IP addresses are used only when the stations are logging in, you only need to provide enough IP addresses to handle simultaneous logins.

You can also configure a **Lease Time** for the temporary address. By default, the lease time is 30 seconds.

When you have configured the address pool, click the **Update** button.

Configure Global Web-Auth Settings—Guest Account



Rev 1.2

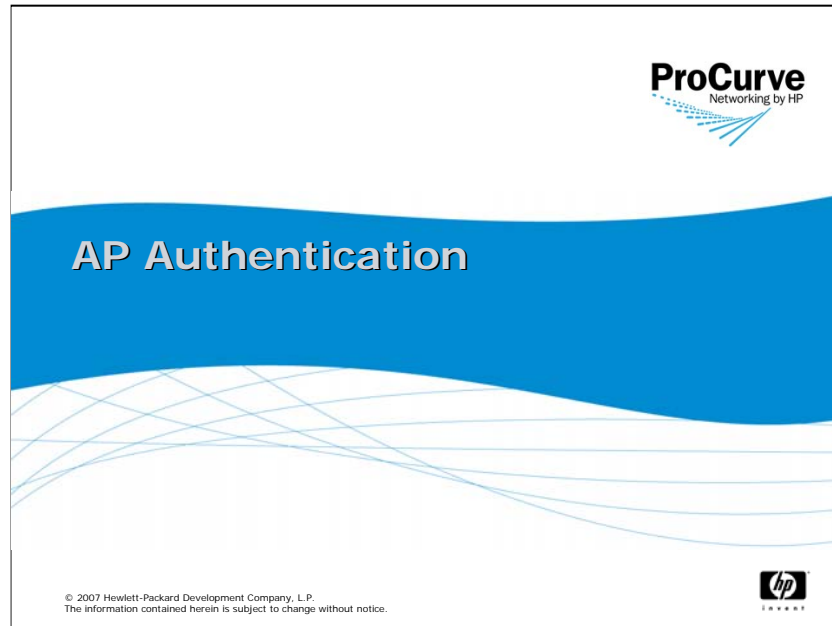
35

Configure Global Web-Auth Settings—Guest Account

There is one other global Web-Auth setting—the Guest Account that is used for Guest Logins. To configure this account, select **Management** > **Web Authentication** > **Guest Account**.

The configuration is quite simple: you enter a username and password and then click **Update**.

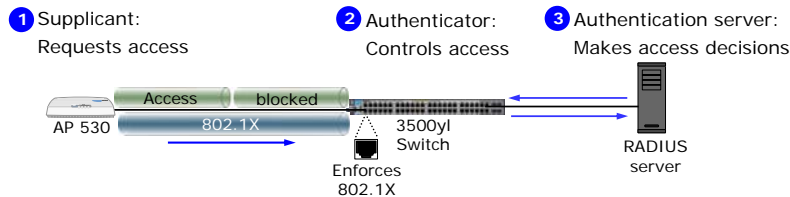
You must then configure a matching account on the RADIUS server you are using to verify login credentials for Web-Auth users. When setting up this account, make sure that the account can have multiple logins.



AP Authentication (802.1X Supplicant)



- You can protect the network from rogue APs by enforcing 802.1X authentication on all switch ports.
- The AP 530 authenticates to the network with its 802.1X supplicant.
- If authentication fails:
 - The AP cannot forward data to the switch.
 - You cannot manage the AP 530 through the Ethernet interface.



Rev 1.2

37

AP Authentication (802.1X Supplicant)

To protect your network, your defenses should begin at the edge. Enforcing port authentication is a key component of edge security. By implementing 802.1X on the ports at your edge switches, you can protect your company's network from rogue APs and other unauthorized devices that can compromise your network security.

The 802.1X authentication process includes three components—the supplicant, the authenticator, and the authentication server. Although you are probably somewhat familiar with this process, you may be accustomed to the AP 530 functioning as the authenticator, rather than as the supplicant. This slide illustrates how the AP 530 functions as a supplicant in this process.

The Supplicant

Simply put, the supplicant (which is also sometimes called the port access entity, or PAE) allows a device to authenticate and then gain access to the network. The supplicant sends the device's login credentials, typically in response to a challenge from the authenticator—in this case, the switch.

With the 2.0 release of the software, the AP 530 now includes a supplicant, allowing it to authenticate to the network.

The Authenticator

The authenticator controls access to the network, forcing a supplicant to authenticate before it can send any non-802.1X traffic over the connection. After initiating the authentication process, the authenticator relays authentication messages between the supplicant and the authentication server, which is typically a RADIUS server. (The AP 530 also functions as an authenticator for WLANs configured with 802.1X.)

The Authentication Server

The RADIUS server makes decisions about whether or not the AP can access the network. These decisions are based on the following:

- The AP can prove its identity. (The supplicant's login credentials are correct.)
- The AP is connecting at the proper time and in the proper location.

After the authentication process is completed, the switch decides how to control the connection. If the RADIUS server approves the AP supplicant's request, the switch begins to accept data from the AP. If the RADIUS server rejects the request, the switch enforces this denial and keeps the connection closed. The AP 530 will be unable to send traffic onto the wired network, and you will be unable to manage the AP 530 through the Ethernet interface, which includes Telnet, HTTP, and SNMP access.

Guidelines for Configuring AP Authentication



- The 802.1X supplicant on the AP 530 supports two Extensible Authentication Protocol (EAP) types:
 - Protected EAP (PEAP)
 - EAP-Message Digest 5 (MD5)
- PEAP is the more secure option.
- The AP's supplicant and the authentication server must be configured to use the same EAP type.
- Your switch must support port authentication.

Rev 1.2

38

Guidelines for Configuring AP Authentication

802.1X uses the Extensible Authentication Protocol, or EAP, for strong, yet flexible, authentication. The AP 530's supplicant supports two EAP types:

- Protected EAP, or PEAP
- Message Digest 5, or MD5

Because PEAP is more secure, you should select this option whenever possible. (MD5 is vulnerable to attacks based on collision-finding techniques. A collision occurs if two files have the same hash. Attackers apply various techniques to create such a collision.)

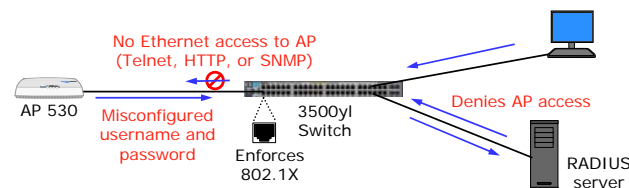
The AP 530's supplicant and the RADIUS server must support the same EAP type, or authentication will fail.

To act as the authenticator, the switch that connects to the AP 530 must support port authentication.

Main Configuration Steps



1. Configure the switch and the RADIUS server to support 802.1X authentication for the AP 530.
2. Configure 802.1X settings on the AP 530 before installing it in its final location:
 - a. Enable the supplicant on the AP 530.
 - b. Select PEAP or MD5 as the EAP type, which must match the type configured on the RADIUS server.
 - c. Specify the username and password, which must match the login credentials stored on the RADIUS server.
3. Test the 802.1X configuration before installing the AP in its final location.



Rev 1.2

39

Main Configuration Steps

To enable port authentication, you must configure the switch and the RADIUS server to support 802.1X authentication for the AP. For this presentation, I will assume that these steps have already been completed and focus on configuring the supplicant on the AP 530. (If you have questions about configuring the switch or the RADIUS server, refer to the appropriate product documentation.)

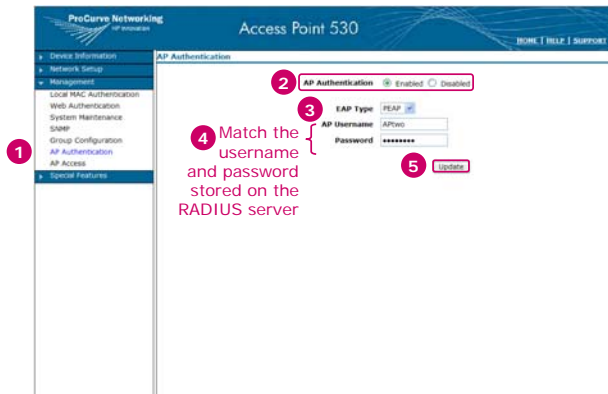
Configuring the 802.1X supplicant on the AP 530 is a simple process: you enable the supplicant, specify the EAP type, and enter the username and password, taking care to match the EAP type and the credentials stored on the RADIUS server.

You should configure and test 802.1X settings on your AP 530 *before* you install the AP in its final location. That way, you can correct any problems that might prevent the AP 530 from connecting to the network—and prevent you from accessing the AP in a difficult-to-reach final location. The example in the slide illustrates what happens if the username and password are misconfigured on the AP 530.

Configure AP Authentication



Select Management > AP Authentication.



Rev 1.2

40

Configure AP Authentication

Select **Management > AP Authentication**, as shown on the slide. In the **AP Authentication** field, select **Enabled** to activate the 802.1X supplicant. To turn the supplicant off, select **Disabled**.

In the **EAP Type** field, use the drop-down menu to select **PEAP** or **MD5**.

In the **Username** field, enter the username you configured on the external RADIUS server. The AP 530 supports usernames and passwords that are between 1 and 32 characters.

In the **Password** field, enter the appropriate password.

Click the **Update** button.

Troubleshoot 802.1X Authentication



View the event log from the AP 530 CLI:

```
ProCurve Access Point 530# show logging
Keys: M=eMergency C=Critical W=Warning I=Information
      A=Alert     E=Error    N=Notice  D=Debug
----- Event Log Listing: Most Recent Events First -----
N 05/02 00:53:16 xsupplicant: md5 failed
N 05/02 00:53:16 xsupplicant: starting authentication
```

EAP method or login credentials may not match those stored on RADIUS server

```
ProCurve Access Point 530# show logging
Keys: M=eMergency C=Critical W=Warning I=Information
      A=Alert     E=Error    N=Notice  D=Debug
----- Event Log Listing: Most Recent Events First -----
N 05/01 00:00:41 xsupplicant: authenticated
N 05/01 00:00:39 xsupplicant: starting authentication
```

Successful login

Rev. 1.2

41

Troubleshoot 802.1X Authentication

If you configure the AP's supplicant and the AP cannot access the network, you can begin troubleshooting the problem by checking the AP 530's log. Because you cannot access the AP 530 through its Ethernet connection, you must set up a serial connection.

Once you access the CLI, you can enter the **show logging** command.

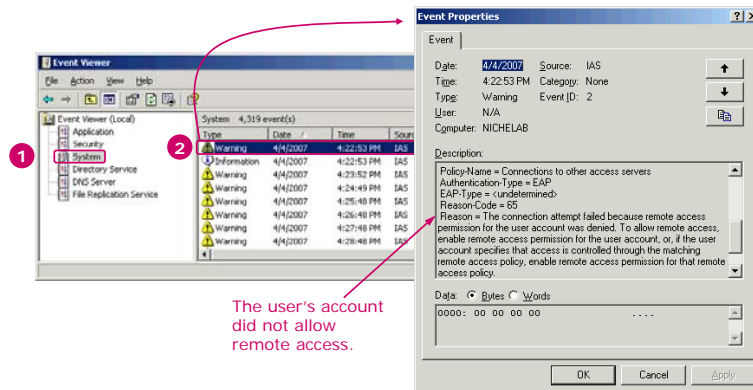
The slide displays the messages logged when 802.1X authentication fails and when it succeeds. If the supplicant reports a failure, you know the problem is not a faulty cable or invalid IP settings. The EAP method configured on the AP 530 may not match the method stored on the RADIUS server, the username and password may be misspelled, or the policy on the RADIUS server may be misconfigured.

For more information about the problem, you can check the RADIUS server itself.

Troubleshoot 802.1X Authentication



- View the event log on the RADIUS server, which controls the authentication process.
- Example—Use the Windows 2003 Event Viewer to see messages for Microsoft Internet Authentication Service (IAS).



Troubleshoot 802.1X Authentication

Because the RADIUS server controls the authentication process, most servers include a log to help you troubleshoot failed attempts to authenticate. For example, this slide shows the Windows 2003 Event Viewer, which contains messages for the Microsoft Internet Authentication Services, or IAS, as well as messages for other Windows 2003 services. IAS is shown because many companies use this RADIUS server.

To access the Windows 2003 Event Viewer, select the **Start** menu and then select **Settings > Control Panel > Administrative Tools**. Double-click the **Event Viewer**.

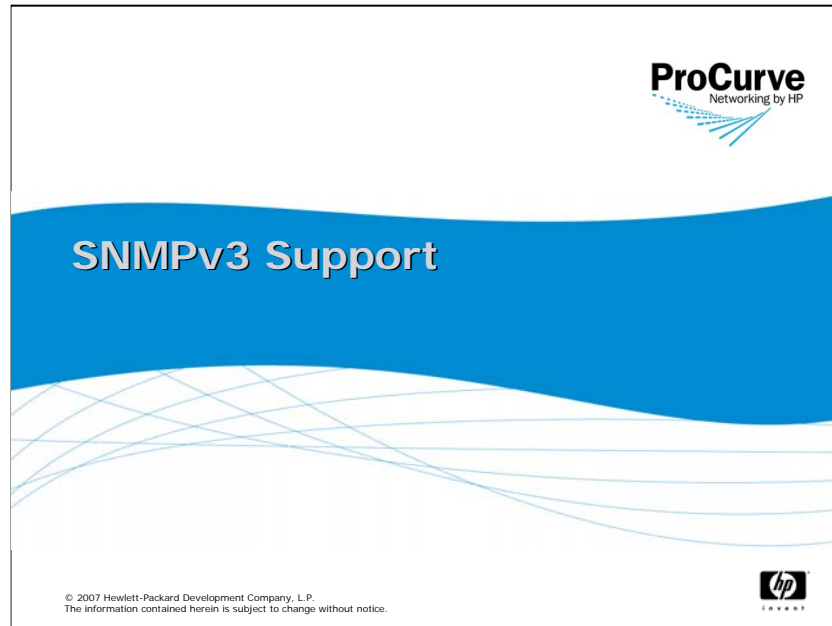
After you open the **Event Viewer**, select **System** in the left pane and scan the most recent messages in the right pane. Identify messages that have IAS as a source. Double-click a message to view it.

In this example, there is a misconfiguration on the RADIUS server: the AP's account does not allow remote access.

Other common problems include:

- Misconfiguration of EAP types—The EAP type configured on the AP 530 does not match the EAP type configured on the RADIUS server.
- Mismatched username and password—The username and password configured on the AP 530 do not match those configured in the RADIUS server's data store.

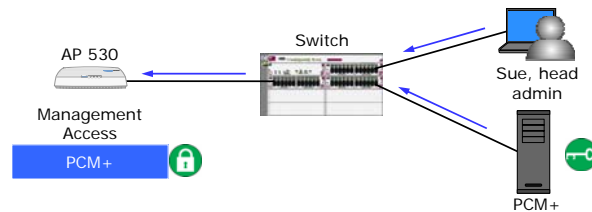
If there are no messages in your RADIUS server's log, you should check the switch's log. The switch may not be able to contact the RADIUS server. Ensure that the switch's 802.1X port authentication settings are correct. In particular, check the RADIUS server's IP address, and if you have configured a shared secret on the RADIUS server, ensure that the secret is entered correctly on the switch as well.



SNMPv3 Support



- SNMPv3 addresses weaknesses in the SNMP framework, making it more secure.
 - Supports authentication and encryption of management traffic
 - Protects traffic from eavesdroppers
- The AP 530 allows you to add up to 10 SNMPv3 users.



Rev 1.2

44

SNMPv3 Support

The AP 530 now supports SNMPv3, which provides a more secure management framework than SNMP versions 1 and 2. SNMPv3 allows you to authenticate SNMP management applications with a username and password and encrypt the data that is exchanged between the managed device—in this case, the AP 530—and the SNMP management console. This encryption protects the communications from eavesdroppers.

You can create up to 10 SNMPv3 users on the AP 530.

SNMPv3 Guidelines



- For SNMP management, the AP 530 must have an IP address and subnet mask.
- You can secure communications between the SNMPv3 user and the AP 530:
 - For authentication, you can select MD5 or SHA.
 - For privacy, you can select DES or AES.

Rev 1.2

45

SNMPv3 Guidelines

The AP 530 allows you to enable and disable SNMPv1/v2 and SNMPv3. SNMPv1 and v2 control traps, so you should usually leave these versions enabled (the default setting). By default, SNMPv3 is also enabled.

When you require authentication for a new SNMPv3 user, you can select either MD5 or Secure Hash Algorithm, or SHA. SHA provides the stronger security, so you should select that option, if possible. If you select MD5 or SHA, you must specify a password.

For privacy (or encryption), you can select Data Encryption Standard, or DES, or Advanced Encryption Standard, or AES. Of the two, AES provides the stronger security. Again, if you select an encryption type, you must specify a password.

Main Configuration Steps



SNMPv3 is enabled by default.

1. Create a new management user.
2. Optionally, select an authentication protocol and configure a password.
3. Optionally, select an encryption protocol and configure a password.

Rev 1.2

46

Main Configuration Steps

SNMPv3 is enabled by default, so you simply need to create the new management user and optionally configure authentication and encryption. The next slides show the configuration screens for SNMPv3.

SNMP Settings Screen



Select Management > SNMP > Settings.

The screenshot shows the 'SNMP - Settings' page in the ProCurve Access Point 530 web interface. The left sidebar (labeled 1) contains a tree view with 'SNMP' selected. The main content area has tabs for 'Settings', 'Tools', 'Top Home', and 'Home'. Under the 'Settings' tab, there are sections for 'SNMPv1/v2c' (with 'Enabled' selected), 'SNMPv3' (with 'Enabled' selected), and 'Engine ID' (displaying '00-00-00-00-00-14-c2-a5-99-33'). Below these are fields for 'Location', 'Contact', and 'Port' (default 161). An 'Update' button (labeled 3) is at the bottom right. Annotations include: 'SNMPv2 communities' pointing to the 'Community Name (R/S)' field; 'SNMPv3 is enabled by default' pointing to the 'SNMPv3' 'Enabled' checkbox; 'AP's location, management contact, and SNMP port' pointing to the 'Location', 'Contact', and 'Port' fields; and 'AP's unique Engine ID' pointing to the 'Engine ID' field.

Rev 1.2

47

SNMP Setting Screen

The **SNMP Settings** screen contains the options to enable or disable all three versions of SNMP. As shown here, all three versions are enabled by default.

The AP's engine ID is listed on this screen as well. SNMPv3 requires each device to have a unique engine ID.

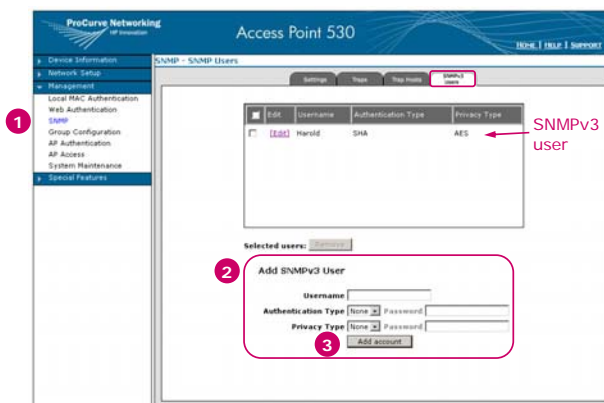
On this screen, you can also configure the location of the AP 530 and the management contact for this AP. These settings are optional, but you may find them useful—particularly, in a large SNMP network. The AP sends this information to the SNMP server, and the SNMP administrator can use the information to locate the device and the person responsible for managing it on a day-to-day basis.

You can also configure the port number the AP 530 should use for SNMP. Unless your SNMP server uses a different port, you should leave this setting at the default—port 161.

Add an SNMPv3 User



Select Management > SNMP > SNMPv3 Users.



Rev 1.2

48

Add an SNMPv3 User

To add an SNMPv3 user, select **Management** > **SNMP** and then select the **SNMPv3 Users** tab. Under the **Add SNMPv3 User** section, enter the new username in the **Username** field.

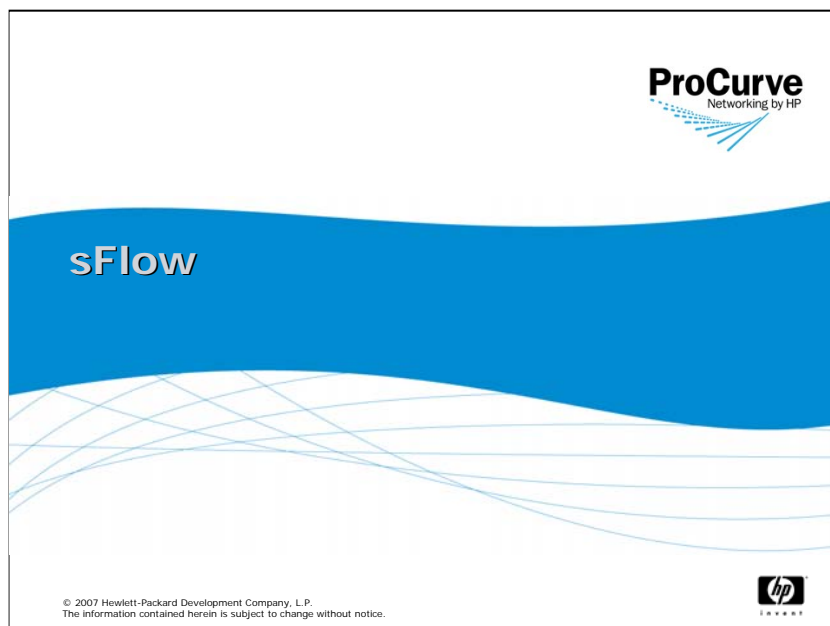
You can then select an **Authentication** method, although SNMP does not require you to do so.

Use the **Authentication Type** drop-down menu to select **MD5** or **SHA**. Then, enter an authentication password.

If you select an authentication type, you can configure encryption. Use the drop-down menu for the **Privacy Type** field to select either **DES** or **AES** and protect communications between the AP 530 and the SNMP management console. Then, enter an encryption password. You can enter the same password for both authentication and encryption, but for tighter security, you should enter different passwords.

Select **Add Account** to commit your configuration to the startup-config. The new SNMPv3 user will be listed in the box above.

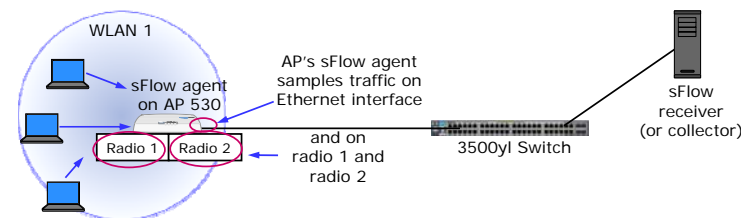
To delete a user, select it in the list and click the **Remove** button.



sFlow—Statistical Sampling



- Two components:
 - sFlow agents—forward traffic samples and counters to an sFlow receiver
 - sFlow receivers (also called sFlow collectors)—collect and analyze samples and counters
- Uses—network troubleshooting, security auditing, and traffic management
- sFlow receivers:
 - ProCurve PCM+
 - ProCurve Network Immunity Manager



Rev 1.2

50

sFlow—Statistical Sampling

Two Components

sFlow is a statistical sampling technology that requires two main components: sFlow agents and sFlow receivers, which are also called *sFlow collectors*. For this presentation, I will use the term *sFlow receivers*.

The AP 530 includes an sFlow agent, which samples a certain percentage of traffic and provides counters to the sFlow receiver. (The next slide describes samples and counters in more depth.) The sFlow agent inspects traffic from its available data sources. As you can see from the example, the AP 530 has three data sources—the Ethernet interface and the two radios. (Incidentally, PCM+ allows you to sample traffic from a subset of the radio interfaces: individual WLANs.)

Uses

After receiving the information the sFlow agent sends, the sFlow receiver analyzes it and creates a statistically accurate profile of network traffic within a margin of error. This profile can be used for network troubleshooting, traffic management, billing, or security auditing by an Intrusion Detection System/Intrusion Prevention System, or IDS/IPS.

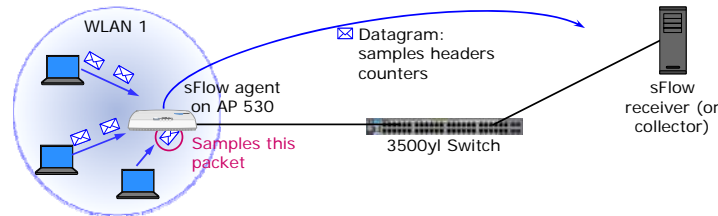
sFlow Receivers

ProCurve Networking offers two solutions that include sFlow receivers—ProCurve Manager Plus (PCM+) and the recently announced Network Immunity Manager.

sFlow Process



- The AP 530's sFlow agent:
 - Uses flow sampling to sample a small percentage of wireless traffic
 - Uses counter polling to track counters of traffic statistics
 - Packages information into datagrams and forwards the datagrams to the sFlow receiver
- The sFlow receiver:
 - Analyzes traffic information from the AP 530 (and other sFlow-enabled devices)
 - Creates a highly accurate picture based on few samples



Rev 1.2

51

sFlow Process

Depending on how you configure sFlow on the sFlow receiver, the AP's sFlow agent can sample a small percentage of traffic or poll interface counters, or—most typically—it can do both.

With flow sampling, the sFlow agent looks at approximately every n th packet and then packages the sampled information into small datagrams. These sFlow datagrams consist of Layer 2 through 7 information, including:

- authentication information
- packet-routing information such as source, destination, and hop addresses
- payload sample—only the header, which is the most important component for traffic analysis

Information from several frames can fit into one datagram.

With counter polling, the AP's sFlow agent periodically polls an interface and requests that it send the counters for traffic statistics. The sFlow agent adds these counters to datagrams. The two types of information work together, and the sFlow receiver combines and analyzes both types of information to create highly accurate statistics.

Because sFlow datagrams are compact and because the sFlow agent samples a small percentage of traffic, sFlow does not require a large amount of network bandwidth. sFlow is extremely scalable: one sFlow receiver can monitor many devices.

Receiver Instances



- The AP 530 sFlow receiver table supports three receiver instances.
- Each instance is configured through the sFlow receiver (via SNMP).



Rev 1.2

52

Receiver Instances

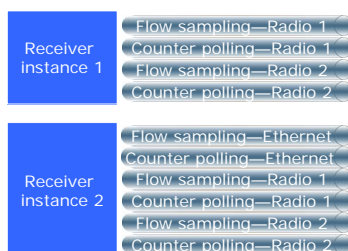
The AP 530 maintains a receiver table with three separate instances. For each of these instances, the sFlow agent forwards datagrams to *one* sFlow receiver, which is said to have reserved that instance. (To actually enable the sFlow agent to create datagrams, the receiver instances must be associated with the appropriate sFlow instances. I'll discuss sFlow instances on the next slide.)

To reserve a receiver instance for a particular sFlow receiver, you configure all the options on the receiver itself. Check the receiver's documentation for more information.

Flow Sampling and Counter Polling



- sFlow instances are configured *per interface* (radios and Ethernet interface):
 - Flow sampling instance, which specifies how often the sFlow agent samples the interface's incoming traffic.
 - Counter polling instance, which specifies how often the sFlow agent polls the interface for statistics.
- The AP 530 supports three flow sampling instances and three counter polling instances per interface.



Rev 1.2

53

Flow Sampling and Counter Polling

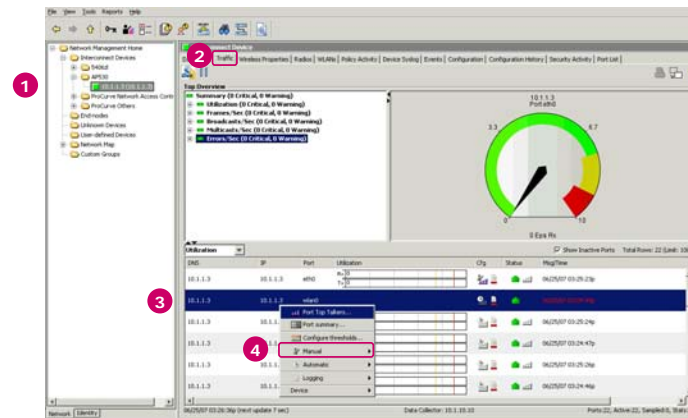
The exact steps vary, depending on the sFlow receiver you are using. But in general, you configure sFlow instances for the AP 530 interfaces—the two radios and the Ethernet interface. The AP 530 supports separate sFlow instances for all of its three interfaces.

For example, the Ethernet's flow sampling instance specifies the sampling rate for traffic that arrives on the Ethernet port. The rate might be 100, which means that the sFlow agent selects, on average, 1 out of every 100 frames. Similarly, the Ethernet's counter polling instance specifies the maximum time that the sFlow agent waits to forward the radio's current traffic counters to the receiver.

The AP 530 supports three of both types of sFlow instances per interface (or data source). Therefore, you can set up flow sampling and counter polling separately for each receiver.

In the example, two of the AP 530's receiver instances are being used.

Example: Configure Flow Sampling Through PCM+



Rev 1.2

54

Example: Configure Flow Sampling Through PCM+

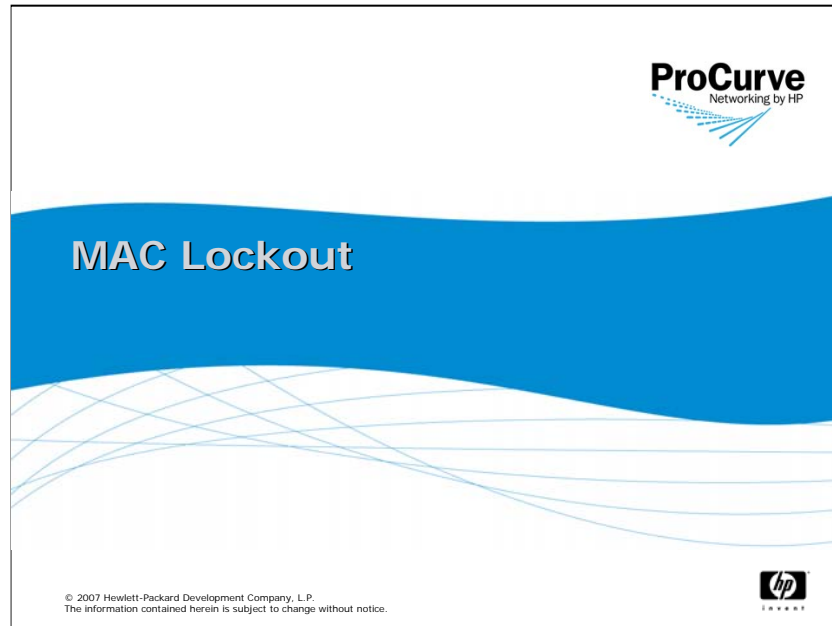
This slide shows how to manually configure flow, or traffic, sampling within PCM+. You first access the PCM **Device tree** and select the appropriate AP 530. Then, select the **Traffic** tab.

At the bottom of the screen, the Ethernet interface and the WLANs are displayed. Select the one on which you want to sample traffic and right-click. When the menu shown above is displayed, select **Manual** > **Manually enable sampling and statistics**.

A dialog box is displayed, asking you to verify that you want this functionality enabled. Click **Yes**.

The sFlow agent on the AP 530 will then begin to sample data and send the results to PCM+. This sampling information allows PCM+ to display reports such as:

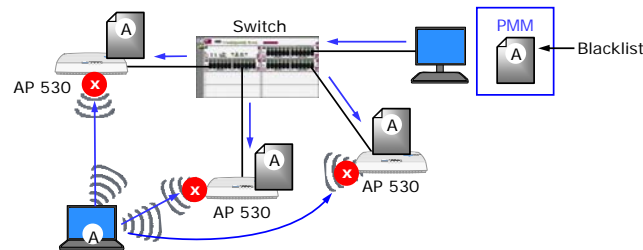
- Port Top Talkers, which identifies the most active devices sending traffic to that data source
- Utilization
- Frames per Second
- Broadcasts per second
- Multicasts per seconds
- Errors per second



MAC Lockout



- Create a blacklist of stations prohibited from your wireless network:
 - Stations on the blacklist are blocked from accessing all WLANs.
 - If you add a station that has associated to a WLAN, the AP 530 forcibly de-authenticates it and prevents it from reconnecting.
- Configure the blacklist:
 - On the AP 530
 - On one AP and use Group Configuration to propagate it other APs
 - On an SNMP server (such as PCM+), which sends it to one or more APs



Rev 1.2

56

MAC Lockout

The MAC lockout feature allows you to create a blacklist of stations that you want to prevent from accessing your wireless network. This blacklist applies to all of the WLANs configured on the AP 530. When stations on this blacklist try to associate and authenticate to any of the AP's WLANs, the AP 530 blocks them. If you add a station that has already associated and authenticated to a WLAN, the AP 530 immediately de-authenticates it and blocks any further attempts that station makes to reconnect.

You have several options for configuring the blacklist. You can use the AP CLI or Web browser interface. If you want to apply the same blacklist to multiple APs, you can use the Group Configuration feature to propagate the list to these APs. (Of course, other parameters are propagated as well.) You can also use an SNMP server to configure the list. The SNMP server—such as PCM+—can send the blacklist to multiple APs. (The MAC lockout feature was added to PCM+ in version 2.2.1.)

MAC Lockout Guidelines



- MAC lockout is always enabled—although the blacklist may be empty.
- The blacklist you create:
 - Can include a maximum of 300 MAC addresses, or stations
 - Takes precedence over local and remote MAC-Auth lists
- If group configuration is enabled on the AP 530, the blacklist is propagated to other group members.

Rev 1.2

57

MAC Lockout Guidelines

The MAC lockout feature is always enabled; you cannot disable it. However, the blacklist may be empty—which in effect disables the feature.

The blacklist can contain a maximum of 300 MAC addresses, or stations.

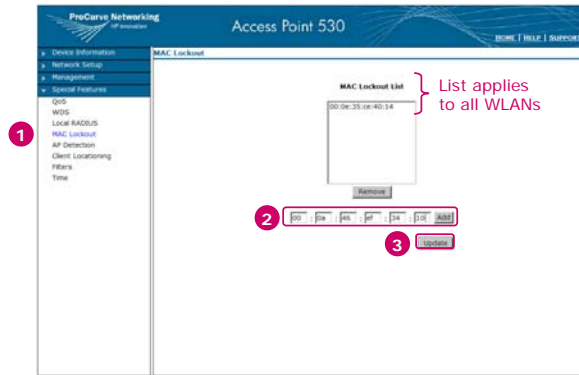
The MAC lockout list takes precedence over local and remote MAC-Auth lists. That is, the AP 530 checks the MAC lockout list before it checks the local and remote MAC-Auth lists, ensuring that a station on the blacklist is not inadvertently granted access to the AP.

As mentioned earlier, if the AP 530 is part of a group configuration, the blacklist is a shared parameter and is propagated to other members in the group.

Configure MAC Lockout



Select Special Features > MAC Lockout.



Rev 1.2

58

Configure MAC Lockout

To configure the blacklist, select **Special Features > MAC Lockout**. Enter the station's MAC address in the six boxes displayed below the list. Then, click the **Add** button. The MAC address you entered is now listed in the **MAC Lockout List**. To save the change to the startup-config, click the **Update** button.

To remove a MAC address from the list, select the address in the **MAC Lockout List**. Click the **Remove** button. Again, you must click the **Update** button to save the change in the startup-config.

View the Event Log



Select Device Information > Event Log.

Station is de-authenticated when its MAC address is added to the blacklist.

Station tries to access the WLAN and is blocked.

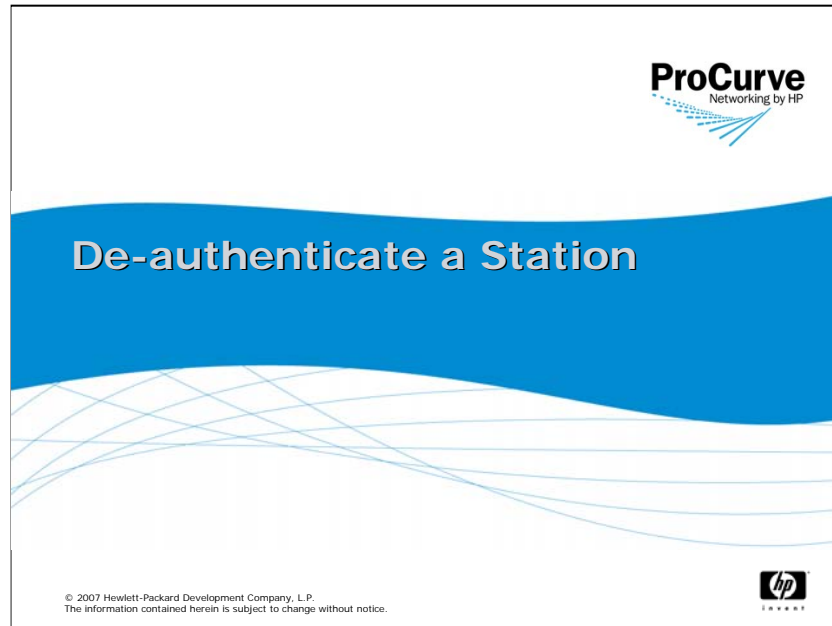
Time	Severity	Event	Message
Jan 9 00:13:12	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:11	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:10	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:10	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:09	warn	Postapd	wlanQueue: STA 00:0e:35:0c:40:14 IEEE 802.11: Locked out station attempting to authenticate
Jan 9 00:13:09	notice	mac lockout	locked out mac address: 00:0e:35:0c:40:14

Rev 1.2

View the Event Log

You can view information about blocked stations in the AP's Event Log, which you access by selecting **Device Information > Event Log**. You can see in this event log, for example, that a station's MAC address was added to the blacklist while the station was associated to a WLAN. The AP 530 immediately de-authenticated the station.

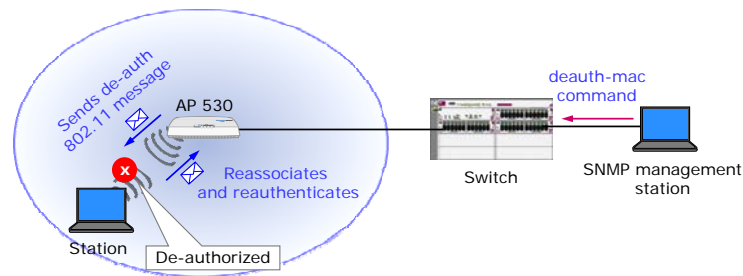
You can also see that although the station's wireless client kept attempting to re-authenticate, the AP 530 prevented it.



De-authenticate a Station



- De-authorizes a station, disconnecting it from the AP one time
- Does not prevent the station from immediately reassociating and reauthenticating to the same WLAN



Rev 1.2

61

De-authenticate a Station

Sometimes you may not want to lock out a station permanently; you may simply want to end its current session. You can use the de-authentication feature to have the AP send a station the following 802.11 message: STA_FAIL_AUTH_TEMPORARILY_DENIED. The station is disconnected one time, but it is then free to re-authenticate.

In practice, you would probably use the de-authentication feature in conjunction with other measures. For example, you might want to change the password for a user's account or force a user to log in with a different username. You would configure these changes on the AP and then de-authenticate the user's station. When the user tried to log in again, the other configuration changes you made would take effect, requiring the user to enter new login credentials.

If you want to permanently block the station from re-associating and re-authenticating to any WLAN, you should use MAC lockout.

Guidelines for Using the De-authentication Feature



- Available through the CLI
- Supported through SNMP, which is typically how the feature will be used

Rev 1.2

62

Guidelines for Using the De-authentication Feature

If you want to use the de-authentication feature, you must do so from the AP 530 CLI or from an SNMP management console. Typically, you will use this feature from an SNMP management console. (This feature is not available from the AP 530 Web browser interface.)

Force a Station to Re-authenticate to the AP



If you do not know the station's MAC address, view the stations associated with the AP:

```
ProCurve Access Point 530# show stations
Station          On WLAN (radio index/WLAN index)  Auth.  Assoc.  Fwd.
-----
00:0e:35:ce:40:14 Marketing (1/2)    Yes    Yes     Yes
```

De-authorize the station:

```
ProCurve Access Point 530# deauth-mac <FF:FF:FF:FF:FF:FF>
```

Example:

```
ProCurve Access Point 530# deauth-mac 00:0e:35:ce:40:14
```

Rev 1.2

63

Force a Station to Re-authenticate to the AP

If you do not know a station's MAC address, you can determine its address by viewing all the stations associated with the AP. From the AP 530 CLI, enter the **show stations** command.

Although the example shows only one station, all the stations associated with the AP will be listed. You can view each station's WLAN, radio, and authentication and association status.

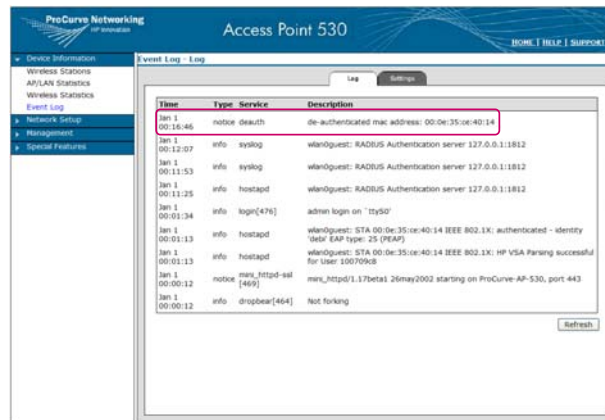
To force a station to re-authenticate, enter the **deauth-mac** command from the enable mode context. Include the MAC address of the station you are forcing to re-authenticate. The command uses the six-colon-delimiter format, as shown in the slide.

Remember that the station will immediately re-authenticate unless you take some other action to prevent it.

View the Event Log



Click Device Information > Event Log.

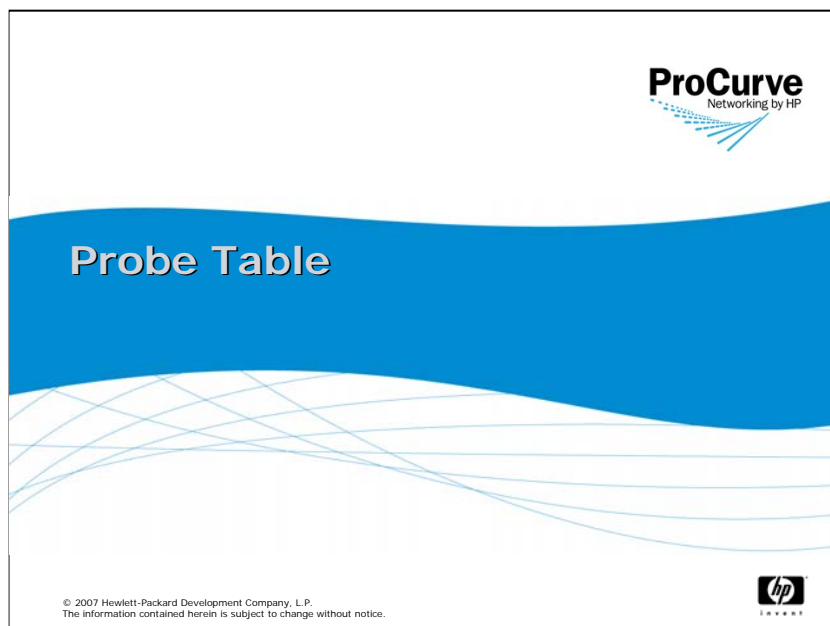


Rev 1.2

64

View the Event Log

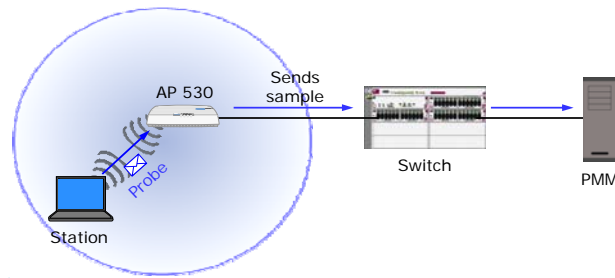
The AP 530 logs an event when it de-authenticates a station, as shown in the slide.



Probe Table



- Probe table allows you to locate and monitor audible stations in SNMP applications such as PMM
- When this feature is enabled, an AP 530 radio:
 - Listens for probe requests from audible stations
 - Packages station information in samples
 - Forwards samples to an SNMP application such as PMM



Rev 1.2

66

Probe Table

The new probe table feature allows you to locate and monitor audible stations (whether or not they are associated with the AP) in SNMP applications such as PMM. This feature complements PMM's rogue AP detection feature, so that you now have the information you need to create a more comprehensive view of wireless activity in your environment.

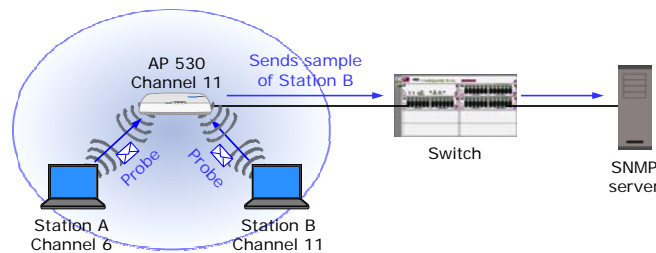
The AP 530 listens for probe requests and gathers information about each audible station. The AP 530 then packages this information in samples and forwards them to PMM.

PMM will then consolidate this information to determine the station's location.

AP 530 Radio with Probe Table Enabled



- Monitors audible stations on its own channel only.
- Tracks the following for each station:
 - Radio number (1 or 2)
 - Station's MAC address
 - Received Signal Strength Indication (RSSI) in dB with no scaling (for antenna gain, for example)
 - Station's transmit power
 - PROBE request SSID



AP 530 Radio with Probe Table Enabled

If the probe table feature is enabled, a radio monitors the audible stations using its own channel. In the example shown in the slide, the radio is using channel 11, so it will gather information about Station B, which is also using channel 11. It will not, however, gather information about Station A, which is using channel 6.

The radio tracks several statistics for each audible station:

- Radio number (1 or 2) for the radio that detected the station
- Station's MAC address
- Received Signal Strength Indication, or RSSI, in dB with no scaling (for antenna gain, for example)
- Station's transmit power
- PROBE request SSID

If the radio cannot discover the station's transmit power, it will use a default value.

PMM (or another SNMP application) will use this information to calculate the station's approximate location.

Probe Table Guidelines



You configure the feature via an SNMP application such as PMM:

- Enable or disable it separately for each radio
- Configure age-out period for table entries

Each radio can monitor up to 512 stations.

Rev 1.2

68

You configure the probe table through the SNMP application. You enable or disable the probe table separately for each radio. By default, it is disabled.

You can also configure the age-out period for the probe table entries. This setting controls how long a station remains listed in the probe table if the AP radio does not detect a new probe from the station.

Each radio can monitor up to 512 stations. Together, the two radios can monitor 1,024 stations.

Summary



Version 2 release adds the following features:

- ATPC maximizes channel coverage and minimizes interference.
- Web-Auth allows users to access a WLAN by authenticating through their Web browser interface.
- Group configuration simplifies deployment and management of multiple APs.
- The AP authentication (802.1X) feature helps you secure your network from the edge.
- SNMPv3 support allows you to tighten security for your SNMP framework.
- The AP's sFlow agent helps you monitor and troubleshoot the wireless network.
- MAC lockout bars certain stations from the wireless network.
- Client de-authentication ends a station's current session, forcing it to re-authenticate to the wireless network.
- The probe table allows you to monitor and track audible stations through an SNMP application.

Rev 1.2

69

The version 2 release adds a number of new features, expanding the AP 530's capabilities but also helping you to configure those capabilities more easily.

With ATPC, an AP radio automatically adjusts its power in response to selected APs to create the best possible coverage area at any given moment.

Web-Auth allows users to authenticate to your network without any annoying setup on their stations. And, with optional encryption and dynamic settings, the AP 530 enforces Web-Auth securely.

Group configuration simplifies deploying and managing multiple APs and is an ideal management tool for small-to-medium businesses.

Enforcing 802.1X port authentication secures your network from the edge. With the new AP Authentication feature, the AP 530 now participates in this secure design.

In addition, the AP 530 now supports SNMPv3, allowing you to tighten security for your SNMP framework.

The AP's sFlow agent—together with an sFlow receiver on a solution such as PCM+ with PMM or Network Immunity Manager—helps you to monitor and troubleshoot the wireless network.

Other security features grant you more control over wireless stations. MAC lockout allows you to completely bar certain stations from accessing any WLAN on the AP 530. Client de-authentication, on the other hand, temporarily de-authenticates a station, forcing it to re-authenticate.

Finally, the AP's probe table capabilities—used in conjunction with a centralized SNMP application—allows you to monitor and track all audible stations in the area.

